IN THIS UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

DOW CORNING CORPORATION, a Michigan corporation,

Plaintiff,

Case No. 15-13781
Hon. Thomas L. Ludington
Magistrate Judge Patricia Morris

v.

ANJANEYULU CHAGANTI and HOMI SYODIA,

Defendants.

_____/

BODMAN PLC
By: Dennis J. Levasseur (P39778)
Jihan M. Williams (P77686)
6th Floor at Ford Field
1901 St. Antoine Street
Detroit, Michigan 48226
dlevasseur@bodmanlaw.com
jwilliams@bodmanlaw.com
(313) 259-7777
Attorneys for Plaintiff Dow Corning Corporation

_____/

AMENDED COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

November 5, 2015

Dow Corning Corporation ("DCC"), by its attorneys, Bodman PLC, for its amended complaint for injunctive relief and other relief against defendants, states as follows:

PARTIES

1. Plaintiff DCC is a Michigan corporation that has its principal place of business located at 2200 Salzburg Street, Midland, Michigan 48640.

2. Defendant Anjaneyulu Chaganti is, upon information and belief, a citizen of Michigan.

3. Defendant Homi Syodia is, upon information and belief, a citizen of Illinois.

JURISDICTION AND VENUE

4. This Court has jurisdiction over this action under 28 U.S.C. §1331 because DCC is asserting a claim under a federal statute, namely, the Computer Fraud and Abuse Act, 18 U.S.C. §1030 ("CFAA").

5. Venue is proper in this Court under 28 U.S.C. §1391 because defendants do business in Bay and Midland Counties, Michigan, and because a substantial part of the events or omissions occurred in this district.

COMMON ALLEGATIONS

A. Relationship Between DCC and Non-Party HCL America, Inc.

6. On or about March 1, 2012, DCC and non-party HCL America, Inc. ("HCL"), which later retained defendants as independent contractors to provide

services to DCC, entered into a certain Master Agreement ("Agreement") under which HCL agreed to provide certain IT services to DCC. See, Exhibit A.

7. Under the Agreement, non-party HCL agreed, among other things, that:

> "**Section 12.01 Ownership and Use of Customer Data**.
>
> "As between the Parties, all Customer Data is and shall remain the property of Customer. Without the prior approval of Customer, to be given in its sole discretion, Customer Data shall not be (a) used by Supplier other than as required to perform the Service, (b) disclosed, sold, assigned, leased, licensed or otherwise provided or made available in any manner to third parties by Supplier, (c) monitored, analyzed, individualized, anonymized, aggregated, stored, or copied by Supplier, or (d) commercially exploited in any form (including any individualized, anonymized, or aggregated form) by or on behalf of Supplier. Any archival tapes containing Customer Data shall be used by Supplier solely for back-up purposes. Supplier hereby does, and shall cause its Affiliates and Supplier Agents to, irrevocably, perpetually and unconditionally assign to Customer without further consideration all rights, title, and interest each may have in any Customer Data, including all intellectual property and other property rights. Such rights shall vest in Customer upon creation of the relevant Customer Data. See, Exhibit A, p. 34.

8. Personal Data is defined in the Agreement as:

> "Personal Data means any Customer Data that identifies or is capable of identifying an individual, or otherwise defined as 'personal information,' 'personal data,' 'sensitive personal data,' 'personal identifiable information,' 'personal health information,' 'non-public

personal information' or similar terms under applicable Laws."

9. With regard to Personal Data, the Agreement provides in relevant part, as follows:

"**Section 12.06 Personal Data.**

"Without limiting the other provisions of this Article, the following provisions apply to Personal Data. If and to the extent that any of the other provisions of this Article purporting to apply to Personal Data conflict with the provisions of this Section, the provisions of this Section shall prevail.

"(a) Other than where expressly requested by an individual data subject, **Supplier shall not use or disclose Personal Data for any purpose other than fulfilling its obligations under the Agreement without the prior approval of Customer and, to the extent required by applicable Law the individual data subject.** To the extent that performance of its obligation hereunder involves, or necessitates the processing of Personal Data, Supplier shall act only on instructions and directions from Customer, including as set forth in the Agreement. Supplier shall promptly comply (which shall in no event be longer than any time frame for compliance required by applicable Law) with any request from Customer with respect to Personal Data that is necessary to allow Customer to comply with applicable Law.

"(b) Supplier shall not disclose Personal Data to any Supplier Agent without the prior approval of Customer and an agreement in writing from the Supplier Agent to use and disclose such Personal Data only to the extent necessary to fulfill Supplier's obligations under the Agreement and for no other purposes.

"(c) Supplier shall process and store all Personal Data in the jurisdiction in which Supplier obtained the data (or, in the case of the Personal Data of data subjects residing in the European Economic Area, in the European Economic Area), and shall not process or store Personal Data in, or transfer Personal Data to, any other jurisdiction without the prior approval of Customer.

* * *

"(f) If Supplier shall have access to 'protected health information' (as such term is defined by the HIPAA Privacy Rule), then if requested by Customer, Supplier shall execute a Business Associate Agreement in a form acceptable to the Parties. The Parties agree to comply with such Business Associate Agreement. In the event of any conflict between the provisions of the Agreement and the provisions of the Business Associate Agreement, the provisions that are more protective of 'protected health information' (as such term is defined by the HIPAA Privacy Rule) shall prevail.

"(g) If any unauthorized or impermissible disclosure, loss of or access to any Personal Data occurs, Supplier shall (i) assist in the identification of affected persons, (ii) allocate call center resources and training to manage inquiries from affected persons, (iii) provide affected persons with credit monitoring services, (iv) assist with the delivery of Customer-provided electronic, hard copy and/or telephonic notifications to affected persons, and (v) take such other actions as may be reasonably required by Customer. If and to the extent that the unauthorized or impermissible disclosure, loss of or access to any Personal Data results from Supplier's acts or omissions, Supplier shall provide the assistance described in clauses(i) through (v) of this subjection at no expense to Customer. If and to the extent that the unauthorized or impermissible disclosure, loss of or access to any Personal Data does not result from Supplier's acts or omissions, Supplier shall provide the assistance described in clauses (i) through (v) of this subjection if and to the

> extent requested by Customer, Supplier's standard, reasonable rate for such resource that is in effect immediately prior to the unauthorized or impermissible disclosure, loss of or access to the subject Personal Data, and shall reimburse Supplier for its Out-of-Pocket Expenses incurred by Supplier at the direction of Customer as a result of Supplier providing such assistance, (A) so long as Supplier informs Customer of the amount of such expenses reasonably in advance of incurring them and (B) provided that Customer may elect that Supplier not provide any such assistance in order to avoid such reimbursement obligation." See, Exhibit A, pp. 36-37; emphasis added.

10. Defendants were Supplier Agents of non-party HCL at all times relevant to this action.

B. Confidentiality of DCC Information.

11. DCC diligently complies with its responsibilities under state and federal law to maintain the confidentiality of information regarding its employees and to protect the privacy of their personal health information and other private information, such as social security numbers and financial information. DCC takes all necessary and required steps to maintain the confidentiality of its employees' Personal Data and related information.

12. To that end, in 2012 both defendants signed a Confidentiality and Inventions Agreement with DCC which provided, among other things, that:

> "[Defendants] acknowledge that certain trade secrets and other confidential information may become known to [defendants] during * * * assignment with Dow Corning. For purposes of this agreement, "Dow Corning" means

> Dow Corning Corporation together with any of its existing or future subsidiaries. * * *
>
> "During the term of [defendants'] assignment with DCC and after termination of this assignment, [defendant] will keep secret all Dow Corning technical and business information and information received by Dow Corning under obligations of confidence and will not reveal or divulge the same to third parties, or use or publish it in any manner, without prior written approval from Dow Corning
>
> * * *
>
> "4. [Defendants] understand and agree that [defendants] [are] liable to Dow Corning for any breach of this agreement and that all of the obligations under this agreement are binding upon [defendants] heirs, assigns and legal representatives." See, Exhibit B.

13. Defendants also signed a Network Computer Usage Agreement with DCC, which provided:

> "[a]ll computer equipment, software, data and supplies that are the property of Dow Corning will be used solely for approved Dow Corning business purposes * * * (2) [defendants] will protect information to which [they] have access from unauthorized disclosure or misuse." See, Exhibit C.

C. Defendants' Unlawful Access and Downloading of Information About DCC's Employees, Former Employees, and Their Dependents.

14. On or about September 24, 2015, DCC learned, based on its use of forensic software, that defendants, who were independent contractors of HCL (or Supplier Agents), had downloaded confidential employee information on their

own USB flash drives from DCC's computers and computer system, to which they had access.

15. Once DCC learned of the data breach, it started (and is still conducting) an investigation to learn about the scope of the breach.

16. To date, DCC has learned that over 4,000 confidential documents (many of which contained embedded files) were downloaded by defendants.

17. To date, DCC has learned that confidential information (including names, social security numbers, addresses and telephone numbers) concerning DCC's employees, former employees, and their dependents downloaded by defendants from DCC's computer system and computers. Some of the information downloaded by defendants was employee financial information, such as retirement calculations, salary information, and bonus calculations.

18. DCC's investigation has determined that the unlawful and unauthorized downloading of the information began sometime in early September 2015. The downloaded documents include current information and also information dating back may years prior to 2015.

19. DCC informed and believes that HCL has talked and met with defendants in an effort to learn about the scope of information downloaded.

20. DCC is also informed and believes that HCL has had limited success in obtaining full cooperation of the defendants.

21. DCC is also informed and believes that neither of the defendants have turned over their laptops or other electronic devices to DCC and/or HCL for forensic analysis to determine the full extent of the information taken and whether any or all of the information was further transferred (via email, for example) to others.

22. DCC has recently learned from HCL that defendants have not turned over all USB flash drives that were used by defendants. By forensic examination of the files DCC obtained from its data loss prevention software, DCC identified the serial numbers of the USB drives defendants used when downloading confidential DCC employee information. Although defendants told HCL that they have returned all USB drives, the returned drives do not correspond with all the serial numbers identified by DCC's software.

23. There is at least one other USB software drive that was used and not returned by defendants.

24. Consequently, DCC believes that defendants are still in possession of at least one USB drive that contains confidential DCC employee information.

25. There was no legitimate reason, contractual or otherwise, for defendants to have to download confidential information and at no time did DCC give permission to defendants to download confidential information. Defendants'

conduct clearly exceeded any authorized access that defendants had to DCC's computers and computer system.

26. DCC has expended significant internal and financial resources, engaged outside attorneys, and hired and retained data security protection for its employees totaling greater than $5,000 in the aggregate.

27. To date, DCC has spent greater than $5,000 in its efforts to investigate the data breach, identify the scope of the breach, and protect its past and present employees and their dependents.

28. Defendants' conduct has caused DCC substantial harm and damages which are continuing.

COUNT I

FOR VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §1030

29. DCC incorporates by reference the allegations in paragraphs 1 through 28 of this amended complaint.

30. DCC's computers and computer system are "computers" as that term is defined in the CFAA. 18 U.S.C. §1030(e)(1).

31. DCC's computers and computer system are "protected computer[s]," as defined in subsection 1030(e)(2) of the CFAA, because they are used in "interstate or foreign commerce or communication."

32. The CFAA prohibits the unauthorized access to and/or use of computers. See, 18 U.S.C. §1030(a)(1)-(7).

33. In particular, subsection 1030(a)(2)(C) of the CFAA prohibits "intentionally access[ing] a computer **without authorization** or **exceed[ing] authorized access**, and thereby obtain[ing] information from any **protected computer** of the conduct involved an interstate or foreign computer." 18 U.S.C. §1030(a)(2)(C); emphasis added.

34. The CFAA defines "exceeds authorized access" as follows: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. §1030(e)(6).

35. As alleged above, defendants accessed and copied data and information from DCC's protected computers to which they were not authorized.

36. Consequently, defendants violated the CFAA.

37. DCC has suffered damages amounting to more than $5,000 in value in the aggregate as defined in the CFAA because it has obtained data security protection for its employees as well as hired other third-parties such as attorneys to investigate and assess the scope of defendants' data breach and potential harm to DCC's past and present employees and their dependents.

38. Subsection (g) of the CFAA provides that:

> "[A]ny person who suffers damage or loss by reason of a violation of this section [to] maintain a civil action against the violator to obtain **compensatory damages** and **injunctive relief** or other equitable relief." 18 U.S.C. §1030(g); emphasis added.

COUNT II

FOR CONVERSION

39. DCC incorporates by reference the allegations in paragraphs 1 through 38 of this amended complaint.

40. DCC has a property right in the information that defendants improperly accessed and downloaded including DCC's confidential information. DCC's property right includes the right to insist that the information not be made available for any unauthorized use and/or disclosure.

41. Defendants have converted that information for their own personal use and benefit without permission or authorization.

42. The value of the information converted by defendants is not possible to ascertain with any reasonable degree of certainty.

43. DCC has demanded that defendants return all information taken by defendants from DCC's computer system so it can protect that information from further unlawful disclosure.

44. DCC believes that defendants have failed to return all information taken.

45. DCC is entitled to an affirmative injunction requiring defendants to give DCC and its representatives complete and unfettered access to defendants' computers and other electronic devices to conduct a forensic review so that DCC can take measures to protect its property from disclosure.

46. As a direct and proximate result of defendants' conversion of DCC's property, DCC has suffered and will continue to suffer immediate and irreparable injury.

COUNT III

BREACH OF FIDUCIARY DUTY

47. DCC incorporates by reference the allegations in paragraphs 1 through 46 of this amended complaint.

48. At all times relevant to this amended complaint, defendants owed DCC a fiduciary duty to protect the information in their possession, and/or to which they had access, from copying, disclosure, dissemination, and/or access to and/or by unauthorized persons.

49. Defendants also owed a fiduciary duty to DCC not to use the information to which they had access except for the purpose which the information was provided to them.

50. Defendants are in breach of their fiduciary duties to DCC by, among other things, their unauthorized copying and downloading of the information described above.

51. As a direct and proximate result of defendants' breaches of fiduciary duty, DCC has suffered and will continue to suffer immediate and irreparable injury.

WHEREFORE, DCC respectfully requests that this Honorable Court grant DCC the following relief:

A. A temporary restraining order, without notice to defendants, that prohibits defendants (as well as others with notice of the order) from taking any steps to transfer, disseminate, erase and/or otherwise destroy or alter any information and/or data (including information and/or data in electronic form) taken from DCC's computers and computer system and ordering defendants to take all reasonable measures, steps and/or efforts to prevent future unauthorized disclosure and/or dissemination of that information;

B. A preliminary injunction that prohibits defendants (as well as others with notice of the order) from taking any steps to transfer, disseminate, erase, and/or otherwise destroy or alter any information and/or data, including information and/or data in electronic form,

taken from DCC's computers and computer system and ordering defendants to take all reasonable measures, steps, and/or efforts to prevent future unauthorized disclosure and/or dissemination of that information.

C. A preliminary injunction that requires defendants to: (1) immediately provide DCC and its agents with complete and unfettered access to all computers and electronic devices (including electronically stored information and email accounts) under defendants' control so that DCC and its agents can conduct forensic examinations; and (2) immediately deliver to DCC and its designated agents all information downloaded by defendants from DCC's computer system and provide a verification, under oath, that all such information has been delivered to DCC;

D. A preliminary injunction that requires defendants to turn over their passports to this Court and/or such other relief that prohibits the defendants from leaving the country during the litigation of this matter;

E. Damages suffered by DCC as a result of defendants' conduct as well as costs and/or attorney fees;

F. Such other and further relief to which DCC is entitled.

Respectfully submitted,

BODMAN PLC

By: /s/ Dennis J. Levasseur
Dennis J. Levasseur (P39778)
Jihan M. Williams (P77686)
6th Floor at Ford Field
1901 St. Antoine Street
Detroit, Michigan 48226
dlevasseur@bodmanlaw.com
jwilliams@bodmanlaw.com
(313) 259-7777
Attorneys for Plaintiff Dow Corning Corporation

November 5, 2015
Detroit, Michigan